

United States District Court

EASTERN

DISTRICT OF

VIRGINIA

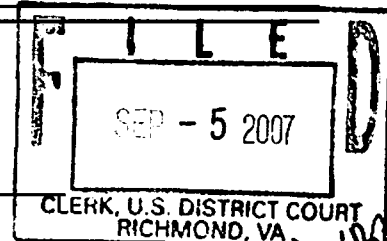
UNITED STATES OF AMERICA

V.

MAX RAY BUTLER

CRIMINAL COMPLAINT

CASE NUMBER: 3:07MJ438



I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief that on or about September 29, 2006, in Richmond, Virginia, in the Eastern District of Virginia, and elsewhere in the jurisdiction of this Court, the defendant did:

[I]ntentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); [or]

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

and attempted to do so, in violation of Title 18 United States Code, Section(s) 1030(a)(2).

I further state that I am a Special Agent of the FBI and that this complaint is based on the following facts:

See attached affidavit.

Continued on the attached sheet and made a part hereof. X Yes No

A handwritten signature in cursive script, appearing to read "Michael R. Schell".

Signature of Complainant

Sworn to before me, and subscribed in my presence

Date

9/5/07

at Richmond, Virginia

City and State

Name and Title of Judicial Officer

/s/
Dennis W. Dohnal
United States Magistrate Judge

AFFIDAVIT FOR CRIMINAL COMPLAINT AND ARREST WARRANT

I. Introduction

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the Richmond Division. I have been employed by the FBI for approximately eight years. I have been involved in investigations of computer related crime for approximately five years. I am currently assigned to investigate cyber-crime in the geographic areas covered by the Richmond Division of the FBI, including the city of Richmond, Virginia and additional surrounding counties. In my capacity as an investigator, I primarily investigate crimes that involve the use of computers and the Internet to commit violations of federal laws through the exploitation of emerging technologies by criminal elements. I have received training and gained experience in the investigation of cyber-crime to include computer intrusion (i.e. "hacking" and "cracking"), crimes against children, extortion, violations of intellectual property rights, identity theft and varieties of computer fraud and abuse schemes to include Internet fraud derived from activities constituting mail and wire fraud.

II. Relevant Statutes

2. Title 18, United States Code, Section 1030(a)(2) provides that whoever—

[I]ntentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); [or]

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

shall be punished as provided in subsection (c) of this section.

3. Title 18, United States Codes, Section 1030(c)(2)(B) provides that in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph the penalty shall be a term of imprisonment for not more than 5 years, or a fine under this title, or both, if—

- (i) the offense was committed for purposes of commercial advantage or private financial gain;

- (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

- (iii) the value of the information obtained exceeds \$5,000...

III. Definitions

4. The term "**computer**" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and any data storage facility or communications facility directly related to or operating in conjunction with such device.

5. The term "**protected computer**" as defined in 18 U.S.C. § 1030(e)(2) means a computer—

- (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

- (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or

communication of the United States...

6. **"Internet Service Providers" or "ISPs"** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
7. An **Internet Protocol address**, also referred to as an **IP address**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
8. A network **"server,"** also referred to as a **"host,"** is a computer system that has been designated to run a specific server application or applications and provide requested services to a "client" computer. A server can be

configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

9. A **"client"** is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.
10. **"Domain Name"** refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first level, or top level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The **Domain Name System**, also referred to **DNS**, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as "www.usdoj.gov," to its currently assigned IP address (i.e., 149.101.1.32), to enable the follow of traffic across the Internet.
11. **"Log Files"** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a

website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

12. **"Hyperlink"** (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
13. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
14. **"Uniform Resource Locator" or "Universal Resource Locator" or "URL"** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
15. **"Webmaster," or "web administrator,"** as used herein, refers to an individual, or group of individuals, that manages the content and functionality of a website that is typically hosted by web servers on the Internet.

IV. Facts and Circumstances

16. This investigation began in October 2006, when representatives of Capital One Services, Inc., (hereafter Capital One) 15000 Capital One Drive, Richmond, Virginia 23238, including Peter Kofira, Director, IT Risk Office, and Tim Joslin, Security Event Management, IT Risk Office, contacted me with information regarding a suspicious e-mail received by over 500 Capital One employees. I know from my training and experience that, for purposes of 18 U.S.C. §

1030(a)(2), Capital One is both a card issuer as well as a financial institution as defined in 18 U.S.C. § 20.

17. Kofira and Joslin indicated that on September 29, 2006, at approximately 7:30 pm, over 500 Capital One employees received a spam email purportedly from GORDON REILY, email address g.reily@lendingnewsgroup.com, with the subject line "CapitalOne customer information leak?" The email contained the following text:

[First Name of Recipient],

I am a reporter for Lending News doing a follow up story on the recent leak of customer records from Capital One. I saw the name [First Name and Last Name of Recipient] in the article from Financial Edge and would like to interview you for a follow up piece.

<http://financialedgenews.com/news/09/29/Disclosure CapitalOne>

If you have time I would greatly appreciate an opportunity to further discuss the details of the above article.

Regards,

Gordon Reily

18. Based upon the number of bounced messages (from recipients who no longer had valid Capital One email addresses), the list of people used to generate the e-mail was six months to one year old. Although Capital One uses a "firstname.lastname@capitalone.com" naming convention for their email addresses, this list was not a random list. The list was built by someone and even in instances where the email address contained only the first initial of the recipient, the body of the message contained the correct first name. The recipients spanned all the departments of Capital One and the Capital One Bank, formerly known as Hibernia Bank. Most of the recipients were either in IT or communications areas. Approximately 25% of the recipients clicked on the link contained in the email.

19. The National Cyber-Forensics and Training Alliance (NCFTA) is joint public/private sector initiative designed to provide a collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement. Your affiant obtained a copy of the exploit files from Capital One network security personnel and provided those files to NCFTA personnel for analysis.
20. The spam claimed that the victim's name was included in the article. The victim was asked to follow a link included in the email to a site (financialedgenews.com) where they would find the article about the leak and upon review Mr. Reilly would like to interview them about the information. Once a victim clicked the link to travel to the supposed news article they would be viewing nothing but a blank page. The page included a malicious script that installed a shell on the victim's computer, allowing the attacker to have complete control over that machine. The term shell refers to a command line interface access to the computer. The attacker could simply use a remote access client, e.g., telnet, to access the infected machine on a port that was hard-coded in the exploit. In addition to being able to remove sensitive data files from the compromised machine, the attacker could also use the victim's compromised machine for anything from spam proxy, phish hosting, malware hosting, dedicated denial of service (DDoS) attacks, etc. The exploit used by the attacker was a well-published VML (Vector Mark-up Language) exploit for Microsoft's Internet Explorer. However, the sender of the exploit successfully modified the malware so that it was far less likely to be detected by antivirus software.

V. Statement of Probable Cause

21. According to Kofira, the link in the body of the email was pulled directly from www.efinancialnews.com to look legitimate. The link for financialedgenews.com connected to IP address 207.234.131.201, which attempted to load the malicious code. That IP address is registered to Affinity Internet, Inc., 3250 W Commercial Blvd. Suite 200, Ft. Lauderdale, FL 33309.
22. According to the publicly available website DNSstuff.com, a site which provides registration information for Internet Domain names and IP addresses, the domain name financialedgenews.com, which was the link in the body of

the e-mail received by Capital One employees, was registered to: Registrant: STEVEN BURBERRY (thomascwik@yahoo.ca), 3559 Salem Rd, Covington, Georgia 20016; Registered through: GoDaddy.com, Inc. (<http://www.godaddy.com>); Domain Name: FINANCIALLEDGENEWS.COM; Created on: 26-Sep-06; Expires on: 27-Sep-07.

23. According to the publicly available website www.domaintools.com, a site which provides registration information for Internet Domain names and IP addresses, the domain lendingnewsgroup.com, contained in the sender's email address in the email which went to the Capital One employees, is registered to: Tessla, Benjamin McFerren, 403 Sand River Ct., Aiken, SC 29801, US, Email: thomascwik@yahoo.ca.
24. According to www.domaintools.com, the Internet Protocol address for financialedgenews.com, 66.98.180.95, resolves to: Everyones Internet, 390 Benmar, Suite 200, Houston, TX 77060.
25. The email was received by the Capital One employees originated from IP address 71.28.181.116, which resolves to, ALLTEL Corporation, 118 E. Gordon Street, Thomaston, GA 30286.
26. According to Keena R. Willis, GoDaddy.com, Inc., 14455 North Hayden Road, Suite 2129, Scottsdale, Arizona, the domain names financialedgenews.org, financialedgenews.com, and financialedgenews.net were registered by Steven Burberry, 3559 Salem Rd, Covington, GA 30016, phone 229-565-8992, email address thomascwik@yahoo.ca, created 9/26/2006 at 9:45:52 PM. The person registering these domain names was assigned GoDaddy.com ShopperID number **10594615**. The person paid using a Visa Credit Card in the name of Steven Burberry and GoDaddy.com recorded IP address 66.67.63.178 as the origination of the transaction.
27. The person using GoDaddy.com ShopperID number **10594615** also registered the domain cardersmarket.com on October 12, 2006, using the following billing information: Wayne Woodhall, 45705 Knightsbrige St, Lancaster, CA 93534, telephone number (613) 812-3358, email address domino8312@yahoo.com. GoDaddy.com recorded IP address 207.44.208.35 at 12:37:52 AM on October 12, 2006, as the registrant's IP address.

28. According to Tracy Jones, Yahoo!, the account for email address domino8312@yahoo.com contained the following information:

Login Name: domino8312
 Properties Used: mail
 Yahoo Mail Name: domino8312@yahoo.com
 (Alternate) Email Address:
 Registration IP Address: 68.5.40.145
 Account Created (reg): Tue Oct 10 05:14:16 2006 GMT
 Other Identities: domino8312 (Yahoo! Mail)
 Full Name: Mr w w
 Address1:
 Address2:
 City: Beverly Hills
 State: CA
 Country: United States
 Zip/Postal Code: 90210
 Phone:
 Time Zone: pt
 Business Name:
 Business Address:
 Business City:
 Business State:
 Business Country: us
 Business Zip:
 Business Phone:
 Business Email:
 Account Status: Active

The account was accessed from the following IP addresses at the following dates and times (all times GMT):

Login	IP Address	Date	Time
domino8312	68.5.40.145	2006-10-10	05:15:19
domino8312	68.5.40.145	2006-10-10	05:20:27
domino8312	69.57.144.8	2006-10-10	18:08:08
domino8312	69.57.144.8	2006-10-11	14:03:39
domino8312	69.57.144.8	2006-10-11	18:25:28

Login	IP Address	Date	Time
domino8312	207.234.185.87	2006-10-16	08:49:02
domino8312	24.122.80.55	2006-10-17	20:35:45
domino8312	207.234.185.87	2006-10-17	21:13:07
domino8312	64.246.56.27	2006-10-17	21:57:45
domino8312	66.98.138.12	2006-10-17	22:59:59
domino8312	207.234.185.87	2006-10-18	14:57:19
domino8312	64.245.56.27	2006-10-19	06:17:57
domino8312	66.98.138.12	2006-10-20	04:00:53
domino8312	207.234.185.87	2006-10-24	15:03:12
domino8312	207.234.185.87	2006-10-24	16:19:44
domino8312	207.234.185.87	2006-10-27	02:36:26
domino8312	207.44.208.35	2006-10-28	21:14:08
domino8312	207.234.185.87	2006-11-07	04:39:01
domino8312	69.203.136.94	2006-11-07	21:08:47

29. Cardersmarket.com is one of multiple criminal Internet websites that have sprung-up over the past several years to provide forums and online meeting places for individuals engaged in criminal carding to negotiate deals and business relationships. "Carding" describes an assortment of activities revolving around the theft and fraudulent use of credit and debit card account numbers, often through Internet-based activities. Related activities include but are not limited to "phishing," computer and network "hacking," "cashing-out" stolen account numbers, Internet auction fraud, and re-shipping schemes. Examples of other such carding sites include www.CCpowerForums.com, www.theftservices.com, www1.mazafaka.ru, and www.darkmarket.ws, among others. Most of these sites require members to register before using, and are generally monitored by site administrators linked to carding activity. While there are differences between these websites, as a general rule they provide some or all of the following services:

- Private and public message posting enabling members to offer and exchange services;
- Tutorials regarding various aspects of carding;
- Downloadable exploits such as source code for phishing web-pages, and hyperlinks to websites providing hacking tools;
- Lists of proxies, which can be used to obscure one's identity on the Internet;
- Areas designated "Hall of Shame," "Scumbags and Rippers," or some other similar designation used to name and ban individuals who rip-off other site members.

30. On October 11, 2006, USA Today published an article regarding online criminal forums, including www.cardersmarket.com, titled "Cybercrime Flourishes in Online Hacker Forums." (Entire article is provided as attachment A). The following is the pertinent text of the article:

...From this post-Shadowcrew milieu, Iceman has emerged as a forum leader to watch.

RSA Security has tracked Iceman's postings on CardersMarket since October 2005; CardCops has compiled an archive of hundreds of postings on several forums by someone using the nickname Iceman since January 2006.

In the boastful world of cybercrime, nicknames, or nics, are sacrosanct. It's not unusual for a hacker or cyberthief to go by two or three different nics, but unthinkable for two or three people to knowingly share the same nic, says RSA Security's Einav. "I believe we're talking about one guy and not a group hiding behind his name," he says.

Hostile takeover

Clearly enterprising and given to posting rambling messages explaining his strategic thinking, Iceman grew CardersMarket's membership to 1,500. On Aug. 16, he hacked into four rival forums' databases, electronically extracted their combined 4,500 members, and in one stroke quadrupled CardersMarket's membership to 6,000, according to security experts who monitored the takeovers.

The four hijacked forums – DarkMarket, TalkCash, ScandinavianCarding and TheVouched – became inaccessible to their respective members. Shortly thereafter, all of the historical postings from each of those forums turned up integrated into the CardersMarket website.

To make that happen, Iceman had to gain access to each forum's underlying database, tech-security experts say. Iceman boasted in online postings that he took advantage of security flaws lazily left unpatched. CardCops' Clements says he probably cracked weak database passwords. "Somehow he got through to those servers to grab the historical postings and move them to CardersMarket," he says.

Iceman lost no time touting his business rationale and hyping the benefits. In a posting on CardersMarket shortly after completing the takeovers he wrote: "basically, (sic) this was long overdue ... why (sic) have five different forums each with the same content, splitting users and vendors, and a mish mash of poor security and sometimes poor administration?"

He dispatched an upbeat e-mail to new

members heralding CardersMarket's superior security safeguards. The linchpin: a recent move of the forum's host computer server to Iran, putting it far beyond the reach of U.S. authorities. He described Iran as "possibly the most politically distant country to the united states (sic) in the world today."

At USA TODAY's request, CardCops traced CardersMarket's point of origin and confirmed that it is registered to a computer server in Iran.

If Iceman succeeds in establishing CardersMarket as the Wal-Mart of forums, its routing through an Iranian server will make an already complex law enforcement challenge that much more difficult, security experts say.

...Trust a thief?

Iceman's masterstroke rattled his rivals and raised suspicions among his peers.

In the tech industry, companies routinely spread what they call FUD – fear, uncertainty and doubt – about a competitor's business model. Shortly after Iceman swept up TalkCash's 2,600 members onto CardersMarket's website, TalkCash's leader, nicknamed Unknown Killer, e-mailed a shrill warning to TalkCash members: "I've talked to a number of guys and all say that they didn't merge a (expletive) with that site ... so please beware as they can be feds."

...Instead of being admired by his peers, Iceman found himself scrambling to deal with an intensifying backlash. A forum member, nicknamed Silo, posted this public comment on CardersMarket: "How Can we TRUST you and this boards admin?"

You breached our community's security.
Stole the Databases of other forums ...
you've breached what little trust
exist's (sic) in the community."

Ten days after the forced mergers, the
deposed leaders of DarkMarket and
ScandinavianCarding managed to
reconstitute forums under those names.
And CardersMarket appeared to be under
assault, with some of the features on
its website functioning sporadically,
according to RSA Security's Einav.

Security experts expect the infighting
to run its course. They say Iceman's
attack prompted forum leaders to beef
up database passwords and patch other
security holes, making both hostile
takeovers and law enforcement
investigations more difficult. Most
experts expect the activity level of
the forums to rise, because many
consumers and businesses are uninformed
or apathetic.

31. According an ongoing undercover FBI operation, the web forum Cardersmarket is owned and operated by a person using the nickname "Aphex." According to an FBI undercover agent active on multiple carding forums, other aliases used by the administrator of Cardersmarket.com include "Digits" and "Iceman." This undercover agent knows from long-term surveillance of carding forums that a person using the nickname "Easylin" was a co-founder of Cardersmarket with "Aphex."
32. Douglas Jackson of e-Gold conducted a database inquiry for any accounts associated with the names "Iceman," "Aphex," or "Digits." Jackson found accounts associated with the nickname "Digits" with the following information:
 - a. E-gold Account number 3143744;
 - b. User name: digits;
 - c. Name: Richard McDaniel;
 - d. Address: 2243 Winona Ave., Montgomery, AL 36107;
 - e. Email address: digits@hush.com.
33. According to their website, www.e-gold.com, "E-Gold is an

electronic currency, issued by E-gold Ltd., a Nevis corporation, 100% backed at all times by gold bullion in allocated storage."

34. Douglas Jackson also linked the above-referenced e-gold Account 3143744 with E-gold account number 3421761 based on a common IP address:

9/2/2006 1:29:47 AM	64.246.56.27	3421761
9/2/2006 1:30:45 AM	64.246.56.27	3143744

35. Information provided by Douglas Jackson for E-gold Account 3421761 revealed the following user registration. 3421761, User: dgt, joe maybe, 321 maple, Chicago, il 60611 email account: amexvisacards4sale@yahoo.com.

36. The IP, 207.44.208.35, used to register the www.cardersmarket.com domain at GoDaddy.com on 10/12/2006 from the same account used in the Capital One Phishing attack is used in multiple times in E-gold Account 3421761.

8/27/2006 18:25	207.44.208.35
8/28/2006 3:05	207.44.208.35
10/13/2006 15:11	207.44.208.35

37. IP Address 64.246.56.27 used in the domino8312@yahoo.com email address on 10/17/2006 is also used multiple times in E-gold Accounts 3143744 and 3421761.

9/2/2006 1:29:00 AM	64.246.56.27	3143744
9/2/2006 1:29:00 AM	64.246.56.27	3421761
9/2/2006 1:30:00 AM	64.246.56.27	3143744
9/2/2006 5:26:00 AM	64.246.56.27	3143744
9/17/2006 3:02:00 PM	64.246.56.27	3421761

38. IP Address 69.57.144.8 used in the domino8312@yahoo.com email address on 10/10/06, 10/11/06, 10/11/06 and 10/20/06 is also used multiple times in E-gold account 3421761.

9/20/2006 3:34:00 PM	69.57.144.8	3421761
9/21/2006 7:05:00 PM	69.57.144.8	3421761
9/21/2006 7:11:00 PM	69.57.144.8	3421761
9/24/2006 6:49:00 PM	69.57.144.8	3421761
9/26/2006 9:14:00 PM	69.57.144.8	3421761
10/1/2006 9:24:00 AM	69.57.144.8	3421761
10/10/2006 11:30:00 AM	69.57.144.8	3421761

39. IP Address 207.234.185.87 used in the domino8312@yahoo.com email address on 10/16/06, 10/17/06, 10/18/06 10/24/06, 10/27/06 and 11/07/06 is also used multiple times in E-gold account 3421761 and 3143744.

8/4/2006 1:56:00 AM	207.234.185.87	3421761
---------------------	----------------	---------

9/8/2006 9:04:00 PM	207.234.185.87	3421761
9/8/2006 9:06:00 PM	207.234.185.87	3421761
9/10/2006 2:03:00 AM	207.234.185.87	3421761
9/10/2006 2:03:00 PM	207.234.185.87	3421761
9/11/2006 11:41:00 AM	207.234.185.87	3421761
9/11/2006 7:06:00 PM	207.234.185.87	3143744
9/15/2006 2:46:00 PM	207.234.185.87	3421761
9/15/2006 5:50:00 PM	207.234.185.87	3421761
9/16/2006 3:48:00 PM	207.234.185.87	3421761
9/18/2006 5:30:00 PM	207.234.185.87	3421761
9/19/2006 11:43:00 AM	207.234.185.87	3421761
10/19/2006 8:15:00 PM	207.234.185.87	3421761
10/20/2006 10:43:00 PM	207.234.185.87	3421761

40. My gCard was a service connected with E-gold in which an ATM card is issued to a user that can be used to withdrawal funds from an E-gold account. The transactions of E-gold account 3421761 reveal withdrawals sent to a My gCard ATM card on numerous occasions.
41. Information provided by Boris Garamond of My gCard revealed the following information concerning the My gCard associated with E-gold account 3421761.

gCard number: 6220983013000104069
 First Name: William
 Last Name: St Patrick
 Phone Number: **(613) 812-3358** and
 E-mail: williamstpatrick@hotmail.com
 Address: 3266 Yonge St, Suite 1220
 City: Toronto
 Country: Canada
 Postal/Zip Code: M4N3P6
 Date of Birth: 08/05/1975
 Driver's License: JF628403
 Passport Country: Canada
 Card number: 6220983013000104069
 Order Number: 1156574996
 Order Date: 2006-08-26 02:49:56

FedEx tracking #: 857073782933

42. In the Capital One phishing attack, the person using the GoDaddy account who also registered Cardersmarket.com used the following billing information:

Wayne Woodhall
 45705 Knightsbrige St. LCA 93534
 Telephone **(613) 812-3358**
 Email Address: domino8312@yahoo.com

43. The phone number on this registration is identical to the one used on the My gCard.
44. On 07/10/2007, pursuant to lawful court order issued in the Eastern District of Virginia, a pen register/trap and trace device was placed on the IP addresses 66.228.114.243 and 208.101.5.90, registered to SoftLayer Technologies, 1950 North Stemmons Freeway, Dallas, Texas 75207. The server bearing these IP addresses was the subject of a search warrant regarding www.cardersmarket.com website in the Northern District of Texas on 05/14/2007.
45. IP address 207.44.208.35, the IP address used to register the www.cardersmarket.com domain name at GoDaddy.com and also used to log into the domino8312@yahoo.com email account, was captured several times by the above-described pen register/trap and trace devices accessing the SoftLayer Technology servers at the following times:
- 7/12/2007 1:10:48 AM to 2:41:37 AM
7/12/2007 2:01:39 AM to 3:09:53 AM
7/12/2007 3:08:02 AM to 3:34:40 AM
8/4/2007 10:12:02 PM to 10:17:15 PM
8/18/2007 8:42:04 AM to 8:59:05 AM
8/18/2007 9:01:42 AM to 10:21:54 AM
8/18/2007 11:53:06 AM to 11:55:55 AM
8/18/2007 12:04:56 PM to 12:17:05 PM
8/25/2007 9:36:05 AM to 10:16:59 AM
8/25/2007 12:13:15 PM to 12:27:44 PM
46. On 03/23/2007, USSS Special Agents interviewed a subject with a great degree of familiarity with Internet-based crimes, including network intrusions, hereafter referred to as Confidential Source (CS) #1. According to CS #1, he began chatting with a person using the email addresses, generous@hush.com and digits@hush.com. This person used the screen names "Iceman," "Darkest," and "Aphex." Through these conversations, CS #1 learned that the person resided in San Francisco, is a vegetarian and possibly has a girlfriend that is a professor. He also thought that this person had family in Portland, OR.
47. CS #1 added that "Iceman" was his source for "dumps." He paid Iceman be sending him reload numbers for Green Dot stored cards. This method allowed CS #1 to charge a Green Dot cards and send that information to "Iceman" who could then have those funds loaded onto his own Green Dot card.
48. "Dumps" is a term used by people involved in online credit

card fraud. The term means information electronically copied from the magnetic stripe on the back of credit or debit cards, including at least Track 2 data, but often Track 1 and Track 2 data. The magnetic stripe on the back of a credit and debit cards has three separate tracks, referred to as "Track 1," "Track 2," and "Track 3." Tracks 1 and 2 collectively will always contain information relating to account numbers and Personal Identification Numbers (PINs), and will often contain such additional information, often in encrypted form, as customer name, Bank Identification Number (BIN) and Credit Card Verification (CCV). Digital information contained in dumps may be encoded onto plastic cards for use in financial transactions such as Automated Teller Machine (ATM) withdrawals.

49. CS #1 stated that after publication of the above-referenced USA Today article, "Iceman" began using the screen name "Aphex."
50. On 4/12/2007, CS #1 stated that he knew the true name of the person using the screen name "Easylin" on cardersmarket.com, and that this person's true initials are "CA." CA is "Iceman's" partner and "runs crews," which entails giving people counterfeit credit cards to make in-store purchases using those cards. They would then sell people those items for 65% of their value.
51. CS #1 stated that CA had introduced him to "Iceman." Additionally, CS #1 stated that a Mongolian girl who uses the screen name "Alenka" had rented an apartment in San Francisco for "Iceman."
52. CS #1 stated that "Iceman's" San Francisco apartment was raided by the FBI in connection with an investigation regarding the hacking of the source code for the game "Half Life 2." According to FBI files, there were two search warrants executed after the theft of the "Half Life 2" source code. The first was executed on 01/16/2004 at 477 Duboce Street, San Francisco, California, the residence of Christopher M. Toshok. The second was executed on 01/20/2004 at 400 Duboce Street, Apartment 208, San Francisco, California, the residence of Max Ray Butler and Charity H. Majors.
53. CS #1 also explained that in the past he received dumps from "Iceman" frequently. Many of these dumps were received through Hushmail, a free encrypted email service. After receiving the dumps CS #1 would pay "Iceman" by sending reloads for Green Dot stored value cards. Stored

value cards like Green Dot are essentially prepaid debit cards that enable purchases only as long as there is a sufficient balance on the card.

54. CS #1 further explained that "Iceman" was able to get the dumps by going to the FDIC web page identifying what banks were insured and then scanning their networks using a vulnerability he had created. "Iceman" primarily targeted smaller banks with this exploit.
55. CS #1 stated that "Iceman" prefers to use wireless networks and one time asked CS #1 to rent him an apartment in San Francisco so that he could place high-powered wi-fi antennas on the roof to trap vulnerable home wireless networks.
56. On 12/22/2005, FBI agents interviewed an individual located in the Orange County Jail in California, hereafter referred to as CS #2. CS #2 stated that in 2002 he was introduced to an individual with the same name and initials CA as identified by CS #1. (Your affiant has no information suggesting that CS #1 and CS #2 know each other.) According to CS #2, CA operated a business called Mission Pacific Leasing. CA had lots of credit profiles that included information such as date of birth, social security number, driver's license, credit report, and bank account information.
57. According to CS #2, CA was looking to obtain credit card information to make counterfeit cards. As a result, CS #2 contacted Max Butler, who he previously knew, about hacking into banks and other places to get credit card numbers. CS #2 met and became friends with Butler while they were serving time at Taft Federal Correctional Institute. Butler was an expert at hacking into computer systems and did time for hacking into Department of Defense records.
58. CS #2 described Butler as a white male, about thirty-years-old and around six feet tall. Butler had a girlfriend Charity Last Name Unknown (LNU) who walks with a limp. Butler and CS #2 communicated with each other via Hushmail.
59. In September or October 2002, CS #2 traveled to San Francisco to meet with CA and Butler. During this visit, Butler, CA, and CS #2 hooked up a large antenna to download data through wireless connections. They were unsuccessful.
60. Later, CS #2, Butler, and CA set up the antenna at CA's residence and were successful in gaining access to records for several credit unions and small banks. Butler was able to obtain extensive information, such as the account

holder's name, social security number, cancelled checks, and any other information that account holder would have through online access.

61. On 02/10/2006, CS #2 was again interviewed by FBI agents. CS #2 advised that an individual named CS #3 was getting credit profiles from CA. CS #3 was using the credit profiles to open bank accounts at off-shore banks.
62. On 10/19/2005, the USSS special agents interviewed an individual with significant familiarity in the area of access device fraud and identity theft, hereafter referred to as CS #3. CS #3 had been arrested on 9/26/2005 trying to purchase designer watches with a counterfeit credit card.
63. According to CS #3, "Max the Hacker" from San Francisco worked with CS #2 and CA in a 2003 credit card scheme developed by CA. CS #3 described Max as six foot five inches tall, 230 pounds, with long brown hair. CS #3 further described Max as approximately 35-years-old and at one time had been hired as a penetrator (i.e., network hacker) for major companies.
64. CS #3 gave \$5,000 to Charity Majors, the girlfriend of Max, to fund the credit card scheme. Within 90 days from the check to Charity Majors, CS #3 met Max. CA initially paid Max \$5,000 to \$10,000 a month, later Max became a 50/50 partner.
65. CS #3 described the scheme as mining of data. They would attack Windows NT systems. CS #3 stated that he acquired high speed internet service for Max in early 2002. CS #3 flew to San Francisco to meet with CA and Max. There they would rent hotel rooms and would hack systems for up to four days. They would point a large antenna from the hotel room or roof and search around for the best signal.
66. CS #3 stated that Max had hacked into 60 million email address. Additionally, CA and Max have a reader/writer able to type up the 16 digit cards.
67. In February 2007, your affiant reviewed a forensic image of the Cardersmarket.com server obtained in June 2006 from the web hosting service provider, Affinity Internet, located in Ft. Lauderdale, Florida. The slack space of the drive contained a message from a person named Alenka to Iceman which indicated Iceman may reside in San Francisco. The message stated:

Hey ICE, I'm back so it looks like I'm

not gonna be doing and EBay works, I am planning to be active on the forum and will try hard to get in contact with maksik. I am planning to post an ad to rent my extra room so where I'm living won't be any work done. I have decided to finish my lease what is to live here in south cali for another 7 months or so. I have talked all about this with dude. Me n dude will be over in SanFran Tuesday next week, so my laptop can get all the work on it done by U.
:D

68. Your affiant knows from training and experience that "maksik," as referenced in Alenka's posted message above, is the online nickname of a notorious large-scale vendor of compromised account numbers and identity information, who is probably located in Ukraine.
69. On 7/2/07, USSS Special Agents interviewed a confidential source of information, hereafter referred to as CS #4. CS #4 advised that she used the online nickname "Alenka." CS #4 stated that in November 2005 she met CA. Your affiant understands that based on name, description and general residence information that the person with the initials CA as identified by CS #4 is the same CA as identified by the other sources of information above. CS #4 stated that CA and his partner, whom she knew as "Sam" (LNU), were creating a website and needed someone to translate and moderate the site. A few weeks later CS #4 moved to southern California to work for CA.
70. CS #4 had spent her days online attempting to befriend Russians who were selling credit card numbers and visiting sites like mazafaka.ru, a Russian criminal forum. In approximately February or March 2006, CS #4 learned the scheme CA was involved in. This scheme involved purchasing fraudulently obtained credit card numbers, manufacturing credit cards with the credit card information purchased, then purchasing and selling goods obtained using the counterfeit credit cards. CA received fraudulently obtained credit card numbers from emails and used that information to manufacture credit cards. CS #4 advised that CA asked here to open a Green Dot card. (Your affiant notes that this is the same method by which Iceman would pay CS #1 as described above.) CS #4 described this

account that money can be deposited into and the cardholder may withdrawal. Sam LNU had a card linked to her account so he was able to withdrawal money that CA put into the account as payment for the dumps provided by Sam LNU.

71. One person CS #4 knew CA to work closely with and the source of numerous credit card numbers was Sam LNU. CS #4 stated that she has never seen Sam LNU in person but has chatted with him online. From her chats with Sam LNU, she learned that he has long hair, has a girlfriend who reads often, and that he is a self-described semi-vegetarian. From information learned from CA, Sam LNU resides in San Francisco and is a well known hacker. CS #4 further learned from CA that Sam LNU was an American and originally from Oregon, and uses the name "Aphex" while working as an Administrator on the forum cardersmarket.com.
72. CS #4 knew Sam LNU to use "Digits" as another online nickname, and CA to use the nickname "Easylivin."
73. According to California DMV records, Max Ray Butler obtained a California driver's license on 8/08/2005, and provided an address of 1241 Stanyan Street, San Francisco, CA, 94117. DMV records further indicate that Butler is 6'5", 220 pounds.
74. On 07/07/2007, USSS Agents conducted surveillance on Max Butler. Surveillance revealed Butler to reside at 73 Webster Street, San Francisco, CA. Butler was described as a white male, approximately 6'5" tall, with long brown hair kept in a pony tail.
75. During the 07/07/2007, surveillance, agents observed Butler transporting and unloading computer equipment from the Webster St. address to 639 Geary St. San Francisco, California. 639 Geary Street is a corporate housing complex named Oakwood/Geary Courtyard.
76. On 07/10/2007, pursuant to lawful court order issued in the Eastern District of Virginia, a pen register/trap and trace device was placed on the IP addresses 66.228.114.243 and 208.101.5.90, registered to SoftLayer Technologies, 1950 North Stemmons Freeway, Dallas, Texas 75207. The server bearing these IP addresses was the subject of a search warrant regarding www.cardersmarket.com website in the Northern District of Texas on 05/14/2007.
77. The pen register/trap and trace device captured logins to

the servers from many IP addresses, including 69.181.236.6 and 68.80.14.77.

78. IP address 69.181.236.6 was captured several times between 07/11/2007 and 07/28/2007. This IP address is registered to Comcast Communications.
79. Comcast Communications records indicate IP address 69.181.236.6, between the dates of 07/11/2007 and 07/28/2007, was assigned to an account in the name of Branden Kin 737 Post Street, Apt. 432, San Francisco, CA 94109.
80. 737 Post Street, San Francisco, California is within one block of 639 Geary Street, San Francisco, California.
81. IP address 66.80.14.77 was captured several times between 08/04/2007 and 08/09/2007. This IP address is registered to MegaPath Networks.
82. MegaPath Networks records indicate that IP address 66.80.14.77, between the dates of 08/04/2007 and 08/09/2007, was assigned to Citi-Net One, 536 Leavenworth Street #1, San Francisco, CA 94109. 536 Leavenworth Street, San Francisco, California is located within one block of 639 Geary Street, San Francisco, California.
83. IP address 70.137.155.103 was captured several times on 07/27/2007. This IP address is registered to AT&T Internet Services.
84. AT&T Internet Services records indicate IP address 70.137.155.103 on 07/27/2007, was assigned to an account in the name of Dong Ha Shin, 737 Post Street, Apartment 331, San Francisco, California.
85. 737 Post Street, San Francisco, California, is located within one block of 639 Geary Street, San Francisco, California.
86. Based on my experience and investigations, I know that it is possible for a user with limited computer skills to obtain access to another person's wireless computer network and appear to originate from the other persons address. I believe the connections from 69.181.236.6, 66.80.14.77, and 70.137.155.103 are indicative of this type of activity.
87. An NCIC record check reveals that Max Ray Butler has a SSN

of 519-84-8144, and a date of birth of 7/10/1972. Among other convictions in his criminal history, Butler was convicted in 2001 for unauthorized access of a computer, in violation of 18 U.S.C. § 1030.

VI. Conclusion

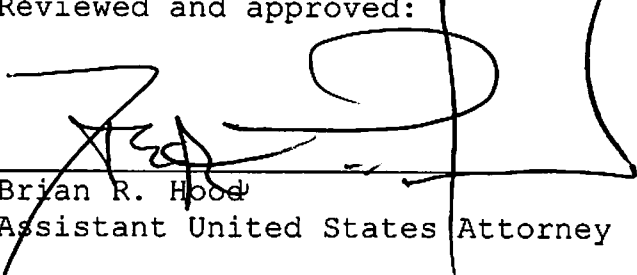
88. Based on the foregoing, I believe that probable cause exists that Max Ray Butler, using the Internet nickname of "Iceman," is responsible for violating Title 18, United States Code, Section 1030(a)(2), for the attempted compromise of the Capital One computer network using the spam-based exploit described above in paragraphs 16-20.
89. Specifically, the person who registered the financialadgenews.com website, which was an integral part of the Capital One attack, also registered the www.cardersmarket.com website according to the domain name registrar GoDaddy.com (paragraphs 26 and 27).
90. According to records from e-gold, the Internet-based currency system, a person using the online nickname "digits" established two e-gold accounts. Those accounts are password protected. One of those accounts, 3421761, was accessed from the same IP address, 207.44.208.35, as was used to register the Cardersmarket.com domain name with GoDaddy.com (paragraphs 27 and 36 above).
91. IP address analysis indicates that on multiple occasions the same IP addresses that were used to access the e-gold accounts established by "digits" were also used to access the email account domino8312@yahoo.com, which was used to register Cardersmarket.com (paragraphs 27 and 37-39).
92. The "digits" person who obtained the My gCard associated with e-gold account 3421761 provided the same telephone number as the person who registered the Cardersmarket.com website (paragraphs 40-43).
93. This same IP address, 207.44.208.35, was detected on numerous occasions by the court-ordered pen/trap device as accessing the Cardersmarket.com criminal forum (paragraph 45 above).
94. CS #1 provided information about a highly skilled hacker known by the Internet nicknames "Iceman" and "Aphex," who lives in San Francisco, CA, with a girlfriend, and who is known to use unsecured wireless Internet access to

perpetrate online crimes. (Paragraphs 41-55) CS #1 communicated with Iceman through several methods, including the email address digits@hush.com, which is the same email address used to establish one of the e-gold accounts listed above (paragraph 32). CS #1 provided information linking the individual he knew as "Iceman" to a previous federal search warrant of Max Butler, who at the time was living in San Francisco, Ca. CS #1 knew "Iceman's" criminal partner to be a man with the initials CA, who used the online nickname "Easylinin."

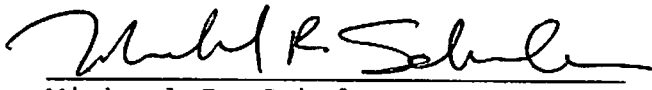
95. CS #2 provided information stating that he knew a highly skilled named Max Butler who lived in the San Francisco, CA, area. CS#2 introduced Butler to CA. The three of them engaged in a variety of Internet-based crimes using equipment to access the Internet through unprotected wireless networks. (Paragraphs 56-61).
96. CS #3 identified an individual named "Max the Hacker" who worked with CA in the San Francisco area. CS#3 worked with CA and "Max the Hacker" to engage in Internet-based crime, including data mining, in part through the exploitation of unsecured wireless networks in the San Francisco area. (Paragraphs 62-66 above.)
97. Forensic analysis of the cardersmarket.com server hosted by Affinity Internet, Ft. Lauderdale, Florida, revealed a private message from person using the online nickname "Alenka" to "ICE" discussing a rendezvous in San Francisco. (Paragraph 67). In July 2007, CS #4 was interviewed by federal agents, and admitted to using the online nickname "Alenka" to communicate with a hacker she knew as "Sam LNU" who used the online nicknames "Iceman," "Aphex," and "Digits." CS#4 reported meeting "Iceman" and CA in San Francisco, and engaging in a variety of activities associated with Internet criminal carding. (Paragraphs 68-72).
98. In July 2007, surveillance by U.S. Secret Service agents of an individual named Max Ray Butler, matching the physical description provided by many of the above-referenced confidential sources, established that Butler was observed loading numerous pieces of computer equipment at the address of 639 Geary St. San Francisco, California. (Paragraphs 73-75).
99. In July 2007, pen register/trap and trace devices

monitoring servers associated with Cardersmarket.com website hosted by SoftLayer Technologies captured numerous accesses to those servers from IP addresses assigned to subscribers physically located within one block of 639 Geary St. San Francisco, California. (Paragraphs 76-85). As noted repeatedly above, Butler appears to be a skilled hacker with a penchant for accessing the Internet from unsecured wireless accounts.

Reviewed and approved:



Brian R. Hood
Assistant United States Attorney



Michael R. Schuler
Special Agent
Federal Bureau of Investigation
Richmond, Virginia

Subscribed and sworn to before me this 5th day of Sept.,
2007.

/s/
Dennis W. Dohnal
United States Magistrate Judge



PRINT THIS

Powered by Clickability

Cybercrime flourishes in online hacker forums

Posted 10/11/2006 10 27 PM ET

By Byron Acohido and Jon Swartz, USA TODAY

SEATTLE — Criminals covet your identity data like never before. What's more, they've perfected more ways to access your bank accounts, grab your Social Security number and manipulate your identity than you can imagine.

Want proof? Just visit any of a dozen or so thriving cybercrime forums, websites that mirror the services of Amazon.com and the efficiencies of eBay. Criminal buyers and sellers convene at these virtual emporiums to wheel and deal in all things related to cyberattacks — and in the fruit of cyberintrusions: pilfered credit and debit card numbers, hijacked bank accounts and stolen personal data.

The cybercrime forums gird a criminal economy that robs U.S. businesses of \$67.2 billion a year, according to an FBI projection. Over the past two years, U.S. consumers lost more than \$8 billion to viruses, spyware and online fraud schemes, *Consumer Reports* says.

In 2004, a crackdown by the FBI and U.S. Secret Service briefly disrupted growth of the forums. But they soon regrouped, more robust than ever. Today, they are maturing — and consolidating — just like any other fast-rising business sector, security experts and law enforcement officials say. In fact, this summer a prominent forum leader who calls himself Iceman staged a hostile takeover of four top-tier rivals, creating a megaforum.

Security firms CardCops, of Malibu, Calif., and RSA Security, a division of Hopkinton, Mass.-based EMC, and volunteer watchdog group Shadowserver observed the forced mergers, as well, and compiled dozens of takeover-related screen shots. "It's like he created the Wal-Mart of the underground," says Dan Clements, CEO of CardCops, an identity-theft-prevention company. "Anything you need to commit your crimes, you can get in his forum."

The Secret Service and FBI declined to comment on Iceman or the takeovers. Even so, the activities of this mystery figure illustrate the rising threat that cybercrime's relentless expansion — enabled in large part by the existence of forums — poses for us all.

In the spy vs. spy world of cybercrime, where trust is ephemeral and credibility hard won, CardersMarket's expansion represents the latest advance of a criminal business segment that began to take shape with the formation of the pioneering Shadowcrew forum.

Shadowcrew, which peaked at about 4,000 members in 2004, arose in 2002. It established the standard for cybercrime forums — set up on well-designed, interactive Web pages and run much like a well-organized co-op. Communication took place methodically, via the exchange of messages posted in topic areas. Members could also exchange private messages.

Shadowcrew gave hackers and online scammers a place to congregate, collaborate and build their reputations, says Scott Christie, a former assistant U.S. Attorney in New Jersey who helped prosecute some of its members.

In the October 2004 dragnet, called Operation Firewall, federal agents arrested 22 forum members in several states, including co-founder Andrew Mantovani, 24, aka ThinkYouPleaseDie. At the time, Mantovani was a community college student in Scottsdale, Ariz. In August, he began serving a 32-month federal sentence for credit card fraud and identification theft.

Attachment A

Advertisement

You'll spend

Sprint ahead

Shadowcrew as catalyst

Shadowcrew's takedown became the catalyst for the emergence of forums as they operate today. With billions to be made, new forums have reformed like amoebas, splintering into 15 to 20 smaller-scale co-ops. "They learned that it's best to disperse," says Yohai Einav, director of RSA Security's Tel Aviv-based fraud intelligence team.

Forum leaders have become increasingly selective about accepting new members. "Vouching" for new members is now the norm, requiring a member in good standing to extend an invitation to new recruits. Some forums charge an initiation fee; others limit the power to invite new members to the forum leaders.

Veteran vendors and buyers typically do business in multiple forums simultaneously, in case any particular forum shuts down.

"If criminals get caught one way, they modify their behavior," says Kevin O'Dowd, an assistant U.S. Attorney in New Jersey who prosecuted the Shadowcrew case.

Some forums have become known for their specialties, such as offering free research tools to do things such as confirming the validity of a stolen credit card number or learning about security weaknesses at specific banks. A few offer escrow services, handling the details of complex deals for a fee.

The better-run forums invest in tech-security measures that have become the norm in the corporate world, such as use of encrypted Web pages. All forums run aggressive campaigns to identify and sweep out rippers — the con artists who gain membership and instigate deals, only to renege on their part of the bargain.

From this post-Shadowcrew milieu, Iceman has emerged as a forum leader to watch.

RSA Security has tracked Iceman's postings on CardersMarket since October 2005; CardCops has compiled an archive of hundreds of postings on several forums by someone using the nickname Iceman since January 2006.

In the boastful world of cybercrime, nicknames, or nics, are sacrosanct. It's not unusual for a hacker or cyberthief to go by two or three different nics, but unthinkable for two or three people to knowingly share the same nic, says RSA Security's Einav. "I believe we're talking about one guy and not a group hiding behind his name," he says.

Hostile takeover

Clearly enterprising and given to posting rambling messages explaining his strategic thinking, Iceman grew CardersMarket's membership to 1,500. On Aug. 16, he hacked into four rival forums' databases, electronically extracted their combined 4,500 members, and in one stroke quadrupled CardersMarket's membership to 6,000, according to security experts who monitored the takeovers.

The four hijacked forums — DarkMarket, TalkCash, ScandinavianCarding and TheVouched — became inaccessible to their respective members. Shortly thereafter, all of the historical postings from each of those forums turned up integrated into the CardersMarket website.

To make that happen, Iceman had to gain access to each forum's underlying database, tech-security experts say. Iceman boasted in online postings that he took advantage of security flaws lazily left unpatched. CardCops' Clements says he probably cracked weak database passwords. "Somehow he got through to those servers to grab the historical postings and move them to CardersMarket," he says.

Iceman lost no time touting his business rationale and hyping the benefits. In a posting on CardersMarket shortly after completing the takeovers he wrote: "basically, (sic) this was long overdue ... why (sic) have five different forums each with the same content, splitting users and vendors, and a mish mash of poor security and sometimes poor administration?"

He dispatched an upbeat e-mail to new members heralding CardersMarket's superior security safeguards. The linchpin: a recent move of the forum's host computer server to Iran, putting it far beyond the reach of U.S. authorities. He described Iran as "possibly the most politically distant country to the united states (sic) in the world today."

At USA TODAY's request, CardCops traced CardersMarket's point of origin and confirmed that it is registered to a computer server in Iran.

If Iceman succeeds in establishing CardersMarket as the Wal-Mart of forums, its routing through an Iranian server will make an already complex law enforcement challenge that much more difficult, security experts say.

"Chasing these carding fraudsters is like chasing terrorists in Afghanistan," says RSA Security's Einav. "You know they are somewhere out there, but finding their caves, their underground bunkers, is almost impossible."

The U.S. Secret Service declined to answer questions about Iceman and CardersMarket. It would not acknowledge whether they are under investigation as part of Operation Rolling Stone, the most intensive federal probe of cybercrime since Operation Firewall. This year, 35

suspects have been arrested. No names were initially released, but a few have surfaced after indictments were unsealed.

Suspects include Binyamin Schwartz, 28, of Oak Park, Mich., indicted in July in Nashville for allegedly trafficking more than 100,000 Social Security numbers, and Paulius Kalpokas, 23, of Lithuania, whose extradition to Nashville on charges of trafficking stolen credit card data has been requested.

Schwartz "got caught up in something on the Internet but did not profit from it," says Sanford Schulman, Schwartz's attorney. "He inquired about acquiring information online without criminal intent, nor was he involved in a sophisticated enterprise."

Secret Service spokesman Thomas Mazur says Operation Rolling Stone is designed to "disrupt and dismantle any of these carding forums," but he declined to say which forums or how many are being investigated.

Security experts worry that CardersMarket's emergence as a model for setting up hypersafe forums could translate into a spike of activity by the best and brightest cybercrooks.

"It's called bulletproofing," says CardCops' Clements. "Guys will now migrate to CardersMarket because they really are untouchable there."

Trust a thief?

Iceman's masterstroke rattled his rivals and raised suspicions among his peers.

In the tech industry, companies routinely spread what they call FUD — fear, uncertainty and doubt — about a competitor's business model. Shortly after Iceman swept up TalkCash's 2,600 members onto CardersMarket's website, TalkCash's leader, nicknamed Unknown Killer, e-mailed a shrill warning to TalkCash members: "I've talked to a number of guys and all say that they didn't merge a (expletive) with that site ... so please beware as they can be feds."

Speculation abounds on the Internet that the FBI helped install Iceman as head of a dominant forum set up to lure kingpin cybercrooks into capture.

In busting up Shadowcrew, law enforcement had used a high-ranking member of Shadowcrew as an inside informant, beginning in August 2003, according to court records. Security experts say it's possible, though unlikely, Iceman could be an informant. While not commenting directly about Iceman, FBI spokesman Paul Bresson says, "The FBI is not in the business of exposing Americans to fraud."

Instead of being admired by his peers, Iceman found himself scrambling to deal with an intensifying backlash. A forum member, nicknamed Silo, posted this public comment on CardersMarket: "How Can we TRUST you and this boards admin? You breached our community's security. Stole the Databases of other forums ... you've breached what little trust exist's (sic) in the community."

Ten days after the forced mergers, the deposed leaders of DarkMarket and ScandinavianCarding managed to reconstitute forums under those names. And CardersMarket appeared to be under assault, with some of the features on its website functioning sporadically, according to RSA Security's Einav.

Security experts expect the infighting to run its course. They say Iceman's attack prompted forum leaders to beef up database passwords and patch other security holes, making both hostile takeovers and law enforcement investigations more difficult. Most experts expect the activity level of the forums to rise, because many consumers and businesses are uninformed or apathetic.

Consumers' lax attitudes

Consumers continue to exhibit lax attitudes, even as Internet intrusions and scams rise in frequency and sophistication. John Thompson, CEO of anti-virus giant Symantec, contends Internet users must adopt the same "sixth sense about security" they use when they get in their cars or leave home.

Meanwhile, the commercial sector has been slow to ask consumers to take other steps, such as using a smartcard or fingerprint reader — along with typing a log-on and password — to prove they are who they say online.

Thomas Harkins spent two decades as operations director for MasterCard International's fraud division, gaining an insider's view of cybercrime's breakneck rise. Now COO of security firm Edentify, based in Bethlehem, Pa., Harkins says identity theft is poised to increase by a factor of 20 over the next two years.

"There's so many stolen identities in criminals' hands that (identity theft) could easily rise 20 times," Harkins says. "The criminals are still trying to figure out what to do with all the data."

Meanwhile, stories such as Kevin Munro's will continue to pile up. In late August, the name, Social Security number and other data of the 51-year-old Warsaw, N.Y., building inspector turned up for sale on a forum monitored by CardCops. Munro recalls changing checking accounts

after a thief tried to cash several bad checks in 2002. Since then, his personal data have persisted in circulation.

Cybercrooks have used it online to order magazines, purchase three Dell computers and attempt to take out a real estate loan. Recently, MasterCard notified Munro that an account he's had for 20 years and uses infrequently was being canceled.

"I work for a living," Munro says. "I do everything on the up-and-up, and some lowlife comes by and takes it away."

Achido reported from Seattle, Swartz from San Francisco.

Find this article at:

http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm

☐ Check the box to include the list of links referenced in the article.

Copyright 2007 USA TODAY, a division of Gannett Co. Inc.